## REMARKS

### Objections

***Objections to the Claims***

The Examiner objected to claim 37 as containing informalities. Applicant has corrected the informalities and respectfully requests the withdrawal of the objection. Applicant further respectfully submits that no new issues are raised by the corrections.

### Rejections

***Rejections under 35 U.S.C. § 103***

**Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, and 40-45**

Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, and 40-45 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,526,506 to Lewis in view of US. Patent No. 6,178,506 to Quick Jr. Both Lewis and Quick qualify as prior art only under 35 U.S.C. § 102(e) because each issued after Applicant's filing date. Applicant does not admit that either Lewis or Quick are prior art and reserves the right to challenge either reference at a later date. Nonetheless, Applicant respectfully submits that the combination does not teach each and every element of the invention as claimed in claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, and 40-45.

Lewis discloses a multi-tiered encryption scheme for a wireless network. The first level of encryption is employed between a mobile device and access points on the network. The second level of encryption is employed between the mobile device and a key distribution server. When a mobile device wants to connect to an access point, the mobile device requests the current network encryption key from the key distribution server. The request and the response containing the network encryption key are encrypted with a master key. The access point can also send a new network encryption key to connected mobile devices in response to the key distribution server changing the network encryption key. The access point encrypts the new network encryption key with the old network encryption key.

Quick discloses a subscription service that is portable among different mobile devices. The mobile devices generates a public/private key pair from the user's

subscription identifier and password. The public key is encrypted with the password. All or part of the unencrypted identifier and the encrypted public key are sent to a local serving system. The local serving system uses the unencrypted identifier to determine the user's home system and sends the encrypted public key to the home system for decryption. The mobile device is authentic if the decrypted public key matches the public key of the user stored on the home system. Further communication establishes the authentication of the home system to the mobile device. Once both ends of the link are authenticated, credentials can be passed to the mobile device to allow it to register with the local server system.

The Examiner is relying on Lewis as disclosing all the elements of Applicant's independent claims, except for what the Examiner states is the claimed encryption of authentication information, which the Examiner asserts is disclosed by Quick. However, Applicant claims that the authentication information is generated using a first key. The Examiner appears to have misread "generating" as "encrypting." Although Quick discloses encrypting the user's public key with the user's password authentication with a key, Quick does not teach or suggest that the user's public key is generated using a key as claimed. In fact, Quick uses the Diffie-Hellman algorithm, which is not key based. Moreover, the Examiner asserts that Lewis' registration information is equivalent to Applicant's claimed authentication but Lewis does not teach or suggest that the registration information is generated using a key.

Furthermore, Applicant claims the interchange of messages between a wireless access point and a station, such as a desktop computer or mobile device, to send a channel key to the station. The station sends a security preference request to the access point, which responds with the appropriate security preference. Applicant's has used the term "security preference" to mean the type of authentication being used to secure the wireless network. The Examiner is respectfully referred to page 10, line 20 through page 11, 7 of Applicant's specification that sets forth one example of a security preference as "shared key." Other types of authentication for wireless networks, such as "open system," may be the security preference for a particular network.

The Examiner is equating Lewis' mobile device with Applicant's claimed station and Lewis' access point with Applicant's claimed access point. However, Lewis only

discloses the exchange of encryption keys, not security preferences as defined by Applicant. Moreover, even if Lewis' encryption key could be properly interpreted as equivalent to Applicant's claimed security preference, Lewis does not teach or suggest that the mobile device receives the new encryption key from the access point in response to the mobile device requesting the key. Instead, Lewis discloses the mobile device receives the new network encryption key from the access point in response to the key distribution server changing the key.

While Lewis discloses that the mobile device requests the current encryption key from the key distribution server upon connection, Lewis describes the key distribution server as separate from the access point. Applicant respectfully reminds the Examiner that it is improper to use two different elements in the prior art as equivalent with a single claim element unless the two prior art elements are known art equivalents. The Examiner has provided no evidence that a key distribution server and a network access point are known equivalents. Unless the Examiner can provide some evidence to support this argument, it must be assumed that the Examiner has improperly relied on Applicant's disclosure to incorporate the functions of Lewis' key distribution server in Lewis' access point. Furthermore, Applicant respectfully points out to the Examiner that the elimination of a prior art element, such as Lewis' key distribution server, while retaining its function in an claimed invention is an *indicia* of non-obviousness [MPEP § 2144.04 II. B.]

Because the combination of Lewis and Quick does not disclose each and every limitation claimed by Applicant for the station and access point in claim 1, the combination cannot be properly interpreted as disclosing the functions of the station and the access point as separately claimed in claims 16 and 26, and claims 21 and 31, respectfully. In addition, the combination cannot be properly interpreted as disclosing a secure wireless network comprising a station and an access point that function as claimed in independent claim 36.

Finally, Applicant respectfully but strongly disagrees with the Examiner's assertion that the rejections of claim 1 can be applied to the message data structure claimed in independent claim 42. Neither Lewis nor Quick disclose a message data structure at all, and therefore cannot be properly interpreted as teaching or suggesting the particular data structured claimed by Applicant.

Accordingly, the combination of Lewis and Quick cannot render obvious Applicant's invention as claimed in claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, and 40-45, and Applicant respectfully requests the withdrawal of the rejection of the claims under 35 U.S.C. § 103(a) over the combination.

**Claims 4-8, 18, 23, 28, 33 and 39**

Claims 4-8, 18, 23, 28, 33 and 39 stand rejected under 35 U.S.C. § 103(a) as being obvious over the combination of Lewis and Quick in view of Schneier ("Applied Cryptography, Second Edition, 1996). Applicant respectfully submits that the combination does not teach each and every element of the invention as claimed in claims 4-8, 18, 23, 28, 33 and 39.

Claims 4-8, 18, 23, 28, 33 and 39 depend from one of independent claims 1, 16, 21, 26, 31 or 36. Because the combination of Lewis and Quick fails to disclose all the elements of the independent claims, Schneier must do so in order to establish a *prima facie* case of obviousness. However, Schneier is directed toward various cryptographic systems and contains no disclosure related to wireless stations or access points as claimed in the independent claims.

Therefore, the combination of Lewis, Quick and Schneier cannot render obvious Applicant's invention as claimed in claims 4-8, 18, 23, 28, 33 and 39, and Applicant respectfully requests the withdrawal of the rejection of the claims under 35 U.S.C. § 103(a) over the combination.

**New Claims**

New claims 46-51 have been added to claim the subject matter of original claims 36-41 under 35 U.S.C. § 112, ¶ 6. Applicant respectfully submits that claims 46-51 are allowable at least for the reasons set forth above for claims 36-41.

## SUMMARY

Claims 1-51 are currently pending. In view of the foregoing amendments and remarks, Applicant respectfully submits that the pending claims are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact Sue Holloway at (408) 720-8300 x309.

**Deposit Account Authorization**

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR
& ZAFMAN LLP

Dated: NOV. 11, 2004

Sheryl S. Holloway
Attorney for Applicant
Registration No. 37,850

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8300 x309